

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Norfolk Division

UNITED STATES OF AMERICA,

v.

Case No. 2:16cr104

LARRY JAMES REECE II,

Defendant

**DEFENDANT'S MOTION TO SUPPRESS**

Comes now the defendant, Larry James Reece II, by counsel and pursuant to Federal Rule of Criminal Procedure 12, and hereby moves this Honorable Court to enter an order suppressing all evidence seized in violation of the Fourth Amendment. On April 15, 2016, the FBI conducted a search of Mr. Reece's house pursuant to a warrant that was 1) unsupported by probable cause, 2) issued based on stale evidence, and 3) supported by an affidavit that was tainted by the material omission of important facts. Mr. Reece asks the Court to suppress all evidence seized during that search as well as the fruits of such evidence.

**QUESTIONS PRESENTED**

**Probable Cause:** Under the Fourth Amendment, warrants must be supported by probable cause. Here, the warrant application alleged that Reece's IP address attempted to access the web address of a popular file sharing service, which itself bore no indicia of child pornography. In other words, someone clicked once on a hyperlink like this: "Click [here](#)." Did that single mouse click—without more—provide probable cause to search Reece's home?

**Staleness:** The Fourth Circuit has held that time is a crucial element of probable cause determinations. Here, the warrant affidavit provided no evidence that anyone was a *collector* of child pornography. It alleged a single attempt to access one illicit file. Does a single incident of attempted access create a fair probability that child pornography will be found in a person's home more than

five months later?

**Material Omissions:** A *Franks* hearing is required upon a preliminary showing that a warrant affiant misled or omitted material facts. Here, the affidavit described a membership-based child porn website, emphasized the proclivities of child porn collectors, implied that Reece accessed a password protected illicit file, and asserted that his email address was used to access child porn. Yet the government had no evidence that Reece ever visited the website, collected child pornography, entered a password, or used an email address. Is a *Franks* hearing warranted?

### **STATEMENT OF FACTS**

On April 5, 2016, the government applied for a warrant to search Mr. Reece's home in Chesapeake, Virginia. (Ex. A, Search Warrant Application.) Homeland Security Special Agent Harald S. Julsrud provided the affidavit in support of the search warrant. Although the affidavit is 14 pages long, only about 1 page describes facts specific to the government's investigation of Mr. Reece.

Much of the affidavit is dedicated to a detailed description of the government's background investigation into a child pornography website referred to as "Bulletin Board A." (Ex. A, ¶¶ 37-45.) According to the affidavit, Bulletin Board A is a website that is dedicated to the advertisement and distribution of child pornography. (Ex. A, ¶ 37.) The affidavit alleges that Bulletin Board A has over 1,500 "approved users." (Ex. A, ¶ 37.) One posting on Bulletin Board A contained a link to a specific child pornography video that is described in Paragraph 40 of the affidavit. To access this video, a Bulletin Board A user had to click on a hyperlink that would send the user to a specific URL where the video file was stored. The URL was associated with a

popular commercial file hosting site: <http://ziifile.com>.<sup>1</sup> Before actually gaining access to the video, however, the user would have to enter a password that was provided in the Bulletin Board A post. (Ex. A, ¶ 39.) According to the affidavit, the Bulletin Board A post contained thumbnail previews of the video and a suggestive filename that included the infamous child pornography catchphrase “pthc.” (Ex. A, ¶ 39.)

Based on this information, it appears likely that someone who landed on this URL by navigating through Bulletin Board A’s posting and clicking on the hyperlink intended to access child pornography. Such a person would have been on Bulletin Board A to begin with—a site dedicated to child porn. Maybe he was even one of the site’s 1,500 approved members. Such a person would have seen the illicit video’s thumbnail previews, and perhaps even caught the reference to ‘pthc’ in the filename, all before clicking the link to access it. But—to be clear—the affidavit never asserts that Mr. Reece’s IP address is associated in any way with Bulletin Board A.

Paragraphs 46-47 of the warrant affidavit provide the only nexus between this illicit video and Mr. Reece’s IP address:

46. The following records were provided by FSS and were associated with the access, download and/or attempted download of file content associated with the following unique URL [http://\[FSS\].com/mkj6j8qjxixb/myuimy5r6yu5e433e.7z.html](http://[FSS].com/mkj6j8qjxixb/myuimy5r6yu5e433e.7z.html).

47. On October 28, 2015, at 5:51:47 PM (17:51:47) Eastern Daylight Time [EDT], IP address 70.161.118.157 was used to download, and/or attempted to download, file content associated with that URL, which as detailed above, consisted of a 49 second video file depicting what appears to be an adult male from the waist down, with his pants pulled down and with an erect penis, and the lower back and buttocks of what appears to be a minor, engaging in sexual intercourse (either actual or simulated) until the adult male ejaculates on the apparent minor’s back and buttocks.

---

<sup>1</sup> Ziifile.com is the file sharing site referred to as “FSS” in the warrant affidavit.

<sup>2</sup> The only apparent reference to this fact is the affidavit’s concession that the IP address may have been used only to *attempt* to download file content associated with that URL. (Ex. A, ¶ 47.)

(Ex. A, ¶¶ 46-47 (emphasis added).) Despite all the talk of Bulletin Board A, the affidavit does not allege that Mr. Reece clicked on any link in Bulletin Board A. It does not allege that Mr. Reece was one of Bulletin Board A’s 1,500 “approved users.” It does not allege that Mr. Reece ever even visited Bulletin Board A. The only allegation is that someone using the Reeces’ IP address navigated to this URL: [http://\[FSS\].com/mkj6j8qjxixb/myuimy5r6yu5e433e.7z.html](http://[FSS].com/mkj6j8qjxixb/myuimy5r6yu5e433e.7z.html).

Unlike the hyperlink posted in Bulletin Board A, this web address contains no catchphrase or indicator that the website being accessed contained illicit content. And although this URL could be accessed by clicking the link in Bulletin Board A, it could also be accessed by clicking any other hyperlink. The affidavit is silent as to how the person using Mr. Reece’s IP address navigated to this URL. Moreover, the affidavit does not allege that the video was either viewed or downloaded by Mr. Reece’s IP address. Indeed—after having established that this video could be downloaded only after entering a password—the affidavit omits the fact that the person using Mr. Reece’s IP address *never entered a password* to access the video.<sup>2</sup> In sum, the affidavit establishes only that Mr. Reece’s IP address navigated one time to this seemingly innocuous URL. The affidavit provides no facts to show that the person using this IP address knew the nature of the website’s contents before navigating to it or that anyone ever actually received illicit content.

The affidavit contains a boilerplate recitation of the “characteristics” of collectors of child pornography writ large. (Ex. A, ¶ 31.) But the affidavit contains no specific facts to support an inference that anyone associated with Mr. Reece’s IP address was a collector of child pornography. Again, the only allegation specific to Mr. Reece’s IP address is the single instance

---

<sup>2</sup> The only apparent reference to this fact is the affidavit’s concession that the IP address may have been used only to *attempt* to download file content associated with that URL. (Ex. A, ¶ 47.)

of attempted access of an illicit video in October of 2015.

On the same day the warrant application was submitted, the magistrate judge signed the warrant authorizing the search of Mr. Reece's home. The search was executed 10 days later, on April 15, 2016. During the search, law enforcement obtained various paper documents, several computers, a camera, a hard drive, and a smartphone. Three months later, on July 21, 2016, Mr. Reece was charged in a four-count indictment with receiving and accessing with intent to view child pornography.

### **ARGUMENT**

The warrant in this case was issued in contravention of the Fourth Amendment for three reasons. *First*, the warrant was not supported by probable cause because the application alleged only that on a single occasion someone using Mr. Reece's IP address navigated to a web address that contained on its face no indicia of child pornography. *Second*, insofar as the Court finds that the facts could have supported probable cause to search Mr. Reece's home in October 2015, these scant facts did not still provide probable cause to search over five months later when the government sought a warrant in April of 2016. *Third*, the affidavit in support of the warrant application contained misleading statements and material omissions, without which the warrant would not have issued. For all these reasons, the search of Mr. Reece's home was conducted in violation of the Fourth Amendment and suppression is appropriate.

**I. A single mouse click on a link to an unsuspecting web address—without more—does not provide probable cause to search a person's home.**

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" and states that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly

describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. “Ordinarily, when a search violates the Fourth Amendment, the fruits thereof are inadmissible under the exclusionary rule, a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect.” *United States v. Doyle*, 650 F.3d 460, 466 (4th Cir. 2011) (internal quotation marks omitted).

Here, the application for the search warrant did not provide probable cause to search Mr. Reece’s home. The affidavit clearly established facts about an illicit posting on Bulletin Board A. The affidavit established that Bulletin Board A was a child pornography site; that Bulletin Board A had 1,500 approved members; that one posting on Bulletin Board A included a link to an illicit video file that was hosted on a popular file sharing site; that the Bulletin Board A posting included thumbnails of the video file and a suggestive filename that included the phrase ‘pthc’; and that the posting contained a password that was needed to actually download the video file from the file sharing site.

But the affidavit contains ***no facts that connect Mr. Reece’s IP address to Bulletin Board A***. This is the affidavit’s critical shortcoming. Rather than connecting Mr. Reece to Bulletin Board A, the affidavit connects Mr. Reece’s IP address only to the ziifile.com web address. To be sure, it is possible that this URL was accessed by clicking on the link posted on Bulletin Board A. But the affidavit provides absolutely no facts to support that assumption. All that the affidavit establishes is that on October 28, 2015, someone using Mr. Reece’s IP address attempted to navigate to this web address: [http://\[FSS\].com/mkj6j8qjixb/myuimy5r6yu5e433e.7z.html](http://[FSS].com/mkj6j8qjixb/myuimy5r6yu5e433e.7z.html). Nothing in this web address indicates that it is associated with child pornography. In fact, the affidavit establishes that the file sharing service—whose name was contained in the

URL—advertises itself as prohibiting not just child pornography, but all pornography. (Ex. A, ¶ 43.) So not only did the name of the web address provide no independent basis for believing that the site contained child pornography—for example, it does not include the letters ‘pthc’—ziifile.com’s service agreement gave an innocent user who clicked on this link reason to believe that the file hosted at that URL did *not* contain pornography of any kind. In sum, the affidavit builds a strong probable cause case against users of Bulletin Board A, but fails to connect Mr. Reece’s IP address to that site. Unless the affidavit is read carefully, it is easy to miss this sleight of hand.

In child pornography cases around the country, courts have consistently emphasized that probable cause to search a person’s home will not be found based on the single click of a computer’s mouse. Particularly analogous facts were addressed by the Second Circuit in *United States v. Coreas*, 419 F.3d 151, 156 (2d Cir. 2005). In *Coreas*, the warrant was supported by allegations that Coreas had clicked on a subscription link after reading the following invitation: “This group is for People who love kids. You can post any type of messages you like too or any type of pics and vids you like too. P.S. IF WE ALL WORK TOGETHER WE WILL HAVE THE BEST GROUP ON THE NET.” *Coreas*, 419 F.3d at 152. The Second Circuit found that probable cause to search was not supported by that single click:

In the view of this panel, that does not remotely satisfy Fourth Amendment standards.... All that Coreas did, so far as the [ ] affidavit shows, was to respond to a three-sentence suggestive invitation from Candyman to join its e-group by clicking a button that added his e-mail address to its roll of members but in no way committed him to partaking in any of its various activities, lawful or unlawful, or even to receiving its e-mails (which he had the option to refuse from the outset). ***The notion that, by this act of clicking a button, he provided probable cause for the police to enter his private dwelling and rummage through various of his personal***

*effects seems utterly repellent to core purposes of the Fourth Amendment.*

*Coreas*, 419 F.3d at 156 (emphasis added). Just as here, there was no problem linking the Candyman group to child pornography. The problem was that the evidence did not sufficiently show that *Coreas* knew that the link he was about to click would give him access to child pornography. At least in *Coreas*, however, the suspect had *some* clue that the link he was clicking was related to kids. As the Second Circuit said, the three-sentence invitation was “suggestive.” *Id.* Here, there is absolutely no evidence as to how Mr. Reece might have come to click on a link that sent him to the facially innocent web address of the ziifile.com file sharing site.

The defense is aware of no case in which a court has upheld a warrant based on the single click of a mouse when the government made no showing that the suspect had some way of knowing what he was clicking on. In *United States v. Gourde*, 440 F.3d 1065, 1070 (9th Cir. 2006), the Ninth Circuit upheld a search warrant when the government did not show any actual downloading of child pornography, but the government had shown that the suspect was the member of a child pornography website. And the government showed that the nature of the website would have been apparent to someone who innocently navigated to the site before becoming a member. *Id.* The Ninth Circuit’s holding was rooted in the fact that the government’s evidence was inconsistent with innocent navigation to the website: “Gourde could not have become a member by accident or by a mere click of a button.” *Id.*

Other courts have relied on the same principle. In *United States v. Payne*, the Third Circuit held that a warrant was supported by probable cause only because the government had shown that the “Defendant could not have undertaken the multi-step process required to join Illegal.CP by accident or with a mere click of a button.” 519 F. Supp. 2d 466, 475 (D.N.J. 2007),

*aff'd*, 394 F. App'x 891 (3d Cir. 2010). *See also United States v. Vosburgh*, 602 F.3d 512, 517 (3d Cir. 2010) (emphasizing that probable cause determination rested on finding that suspect had to have taken several steps because “[a] user seeking to access a link to child pornography posted on Ranchi cannot do so with a simple click of the mouse”); *United States v. Diaz*, 529 F. Supp. 2d 792, 799 (S.D. Tex. 2007) (distinguishing from situation “where the defendant was only required to click on a subscribe link”); *United States v. Kreitzer*, No. 3:12-CR-133, 2013 WL 3479245, at \*9 (S.D. Ohio July 10, 2013) (contrasting facts that presented probable cause with an “innocuous” link “that an unsuspecting user might click on, only to be confronted with a pornographic image containing a child”).

A single click on a hyperlink to a web address that on its face contains nothing indicative of illegal activity cannot possibly support probable cause to search a person’s house. The link to this web address could have appeared anywhere in any form. “Each day, billions of unsolicited email messages are sent over the Internet.” *United States v. Kelley*, 482 F.3d 1047, 1055–56 (9th Cir. 2007) (Thomas, J., dissenting). This link could have appeared in an email. Or it could have appeared on some other website. Clicking on any of the three items below, would send someone to the web address in question:<sup>3</sup>

[www.cnn.com/2016-politics/ClintonEmails/Comey//77382.html](http://www.cnn.com/2016-politics/ClintonEmails/Comey//77382.html)



*Click Here for good times!*

<sup>3</sup> The actual links appear here as they appear in the warrant affidavit, using the [FSS].com introduction rather than the ziifile.com introduction of the actual web address. Accordingly, the hyperlinks here will not actually cause a reader of this motion to navigate to any working web address in the event of an inadvertent mouse click.

Without more, the fact that someone using Mr. Reece's IP address attempted to access the URL of a popular file sharing service, which itself bore no indicia of child pornography, does not provide probable cause to search Mr. Reece's home. Because the warrant was not supported by probable cause, the search of Mr. Reece's residence violated the Fourth Amendment.

**II. Absent some evidence of “collecting” behavior, an isolated, unsuccessful attempt to access one illicit video over the internet does not provide probable cause to search a person's home over five months later.**

Even if the Court finds that the facts in the warrant application supported probable cause to search Mr. Reece's home in October of 2015, this evidence was stale by time the government applied for the warrant over five months later.

The Fourth Circuit has explained that the Fourth Amendment “bars search warrants issued on less than probable cause, and there is no question that time is a crucial element of probable cause.” *United States v. McCall*, 740 F.2d 1331, 1335-36 (4th Cir. 1984). “A valid search warrant may issue only upon allegations of ‘facts so closely related to the time of the issue of the warrant as to justify a finding of probable cause at that time.’” *Id.* (quoting *Sgro v. United States*, 287 U.S. 206, 210-11 (1932)). “Consequently, evidence seized pursuant to a warrant supported by ‘stale’ probable cause is not admissible in a criminal trial to establish the defendant's guilt.” *McCall*, 740 F.2d at 1336.

There are two sets of facts that raise staleness issues: those where the facts were sufficient to establish probable cause when the warrant was issued but the government's delay in executing the warrant tainted the search; and those where the warrant itself is suspect because the information on which it rested was too old to furnish “present” probable cause. *See McCall*, 740 F.2d at 1336. This case presents the second type of staleness issue—where the information on

which the warrant rested was too old to furnish ‘present’ probable cause. “To determine staleness, the court must examine all relevant facts and circumstances, including ‘the nature of the unlawful activity alleged, the length of the activity, and the nature of the property to be seized.’” *United States v. Washington*, 139 F. App’x 479, 482 (4th Cir. 2005) (quoting *McCall*, 740 F.2d at 1336).

Here, the warrant application alleged only a single instance in which someone using Mr. Reece’s IP address attempted to access a web address that contained illicit content. This incident occurred on October 28, 2015. (Ex. A, ¶ 47.) The government did not apply for the warrant to search Mr. Reece’s house until April 5, 2016—over five months later.

A broad range of items were to be seized pursuant to the warrant, but they consisted mostly of electronic equipment and computers. (Ex. A, Attachment B.) To be sure, the warrant application indicates that computer files “can be recovered months or even years after they have been downloaded onto a hard drive.” (Ex. A, ¶ 36.) But the affidavit does not establish that anyone using Mr. Reece’s IP address actually downloaded or viewed any illicit files. So the nature of the items seized cuts neither for nor against the staleness argument here. While the affidavit establishes that once files are saved on a computer they can be recovered later, the affidavit provides no evidence that any illicit files were ever actually saved on or accessed by a computer utilizing Mr. Reece’s IP address.

The length of the activity alleged demonstrates that the evidence supporting probable cause was stale. The activity alleged was a single instance of attempted access. Thus, the alleged activity lasted a fraction of a second. The affidavit does not allege that the video file was ever even successfully viewed, let alone downloaded, saved, and stored on any computer located at Mr.

Reece's home.

Finally, the nature of the activity alleged demonstrates the staleness of the government's evidence. To be sure, the affidavit discusses the characteristics of child pornography collectors in the abstract. (Ex. A, ¶ 31.) But the affidavit contains no facts suggesting that Mr. Reece was a collector of child pornography. Thus, the affidavit's assertion that "[c]ollectors of child pornography prefer not to be without their child pornography for any prolonged period of time," can be accepted as true by the Court but is still entirely meaningless to the probable cause determination here. (*Id.*) The affidavit again provides a detailed description of facts that would be relevant only if the affidavit in some way connected them to Mr. Reece or his IP address. Absent that nexus, many of the facts and assertions contained in the affidavit are simply irrelevant.

The Second Circuit recently held that a warrant was not supported by probable cause in a case very similar to this. *See United States v. Raymonda*, 780 F.3d 105, 116–17 (2d Cir.), *cert. denied*, 136 S. Ct. 433 (2015). In *Raymonda*, the Second Circuit acknowledged that "the determination of staleness in investigations involving child pornography is 'unique'" because "it is well known that images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes, [so] evidence that such persons possessed child pornography in the past supports a reasonable inference that they retain those images—or have obtained new ones—in the present." *Id.* at 114 (internal quotation marks omitted). "Crucially, however, the value of that inference in any given case depends on the preliminary finding that the suspect is a person 'interested in' images of child pornography." *Id.* "The alleged 'proclivities' of collectors of child pornography, that is, are only relevant if there is probable cause to believe that a given defendant *is* such a collector." *Id.* (internal quotation marks omitted).

In *Raymonda*, the affidavit did not demonstrate that the defendant was a collector of child pornography. The court explained:

[T]o establish probable cause in this case, where the agents applied for a warrant on the basis of nine-month-old evidence, it was not enough simply to show that the suspect had at some point accessed thumbnails of child pornography. It was necessary to show that he accessed them in circumstances sufficiently deliberate or willful to suggest that he was an intentional “collector” of child pornography, likely to hoard those images—or acquire new ones—long after any automatic traces of that initial incident had cleared. No such propensity-raising circumstances are present in the record. Agent Ouzer’s affidavit alleged only that, on a single afternoon more than nine months earlier, a user with an IP address associated with Raymonda’s home opened between one and three pages of a website housing thumbnail links to images of child pornography, but did not click on any thumbnails to view the full-sized files. The affidavit contained no evidence suggesting that the user had deliberately sought to view those thumbnails or that he discovered [www.coolib.org](http://www.coolib.org) while searching for child pornography.... Nor was there any evidence that the user subsequently saved the illicit thumbnails to his hard drive, or that he even saw all of the images, many of which may have downloaded in his browser outside immediate view. Far from suggesting a knowing and intentional search for child pornography, in short, the information in Agent Ouzer’s affidavit was at least equally consistent with an innocent user inadvertently stumbling upon a child pornography website, being horrified at what he saw, and promptly closing the window.

Under those circumstances, *absent any indicia that the suspect was a collector of child pornography likely to hoard pornographic files, we hold that a single incident of access does not create a fair probability that child pornography will still be found on a suspect’s computer months after all temporary traces of that incident have likely cleared.* We thus conclude that the warrant issued in this case was not supported by probable cause.

*Raymonda*, 780 F.3d at 116–17 (footnote omitted) (emphasis added). At least in *Raymonda*, the government had shown that the IP address in question actually accessed child pornography, albeit in thumbnail form. Here, the affidavit established only that someone using Mr. Reece’s IP

address navigated to the file sharing site web address, was prompted for a password before viewing any substantive content, and when so prompted clicked away and exited out to close the screen.

The defense submits that the affidavit here does not establish that probable cause ever existed to search Mr. Reece's home. But insofar as the scant facts here ever gave rise to probable cause, the passage of over five months between the single instance of alleged attempted access and the application for a warrant rendered the factual basis for the warrant stale. For that reason, the search of Mr. Reece's home violated the Fourth Amendment.

**III. By emphasizing the proclivities of child pornography collectors and the inflammatory investigation into Bulletin Board A while omitting critical facts demonstrating the missing nexus between these subjects and the Reece's residence, the affiant misled the magistrate.**

In *Franks v. Delaware*, 438 U.S. 154, 156 (1978), the Supreme Court held that "where the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request."

The doctrine applies to omissions, not just false statements. *United States v. Colkley*, 899 F.2d 297, 300 (4th Cir. 1990); *see also United States v. Eccleston*, 615 F. App'x 767, 780 (4th Cir. 2015). *Franks* relief may also be justified when the "agents' failure to verify readily available information amount[s] to a reckless disregard for the truth." *In re Search Warrants Served on Home Health & Hospice Care, Inc.*, 121 F.3d 700 (4th Cir. 1997) (unpublished). And the doctrine further applies when the affiant intentionally or recklessly omitted facts required to prevent technically true statements in the affidavit from being misleading. *See United States v.*

*Tate*, 524 F.3d 449, 456-57 (4th Cir. 2008). If an omission or statement is recklessly or intentionally false or misleading the court must determine if the offending inaccuracy is “material” to the probable cause determination. “To determine materiality, a court must excise the offending inaccuracies and insert the facts recklessly omitted, and then determine whether or not the ‘corrected’ warrant affidavit would establish probable cause.” *Miller v. Prince George’s Cty.*, 475 F.3d 621, 628 (4th Cir. 2007) (internal quotation marks omitted).

Here, a Franks hearing is required based on several misleading statements and omissions contained in the affidavit. **First**, the affidavit asserts that the child pornography video hosted on the file sharing site was password protected, but the affidavit omits the fact that the person who allegedly navigated to the file sharing site from Mr. Reece’s IP address ***never entered a password***. This is critical to the probable cause issue. The affidavit already leaves open the question whether Reece accessed the file sharing site via Bulletin Board A. But a judge reading the affidavit knows that the post on Bulletin Board A contained the file sharing site’s URL and the password to access the video. So if someone navigated to the file sharing site but did not enter the password, it suggests that this person did not navigate to the file sharing site through Bulletin Board A—otherwise, he would have known the password and entered it.

**Second**, the affidavit is misleading because it contains a detailed, boilerplate description of the characteristics of child pornography collectors without any evidence that Mr. Reece (or anyone else in his home) was a collector of child pornography. In *Raymonda*, Judge Chin wrote separately to acknowledge the impropriety of similar boilerplate allegations when the evidence to support collection was even stronger than it was here. There the evidence “only showed that Raymonda had opened the coollib.org webpage, whether purposely or inadvertently, some nine

months earlier, and that he may have viewed—without clicking on—the thumbnail sketches and that there was activity for a period of no more than 17 seconds.” *Raymonda*, 780 F.3d at 124 (Chin, J., concurring in part and dissenting in part). Judge Chin concluded, “Without any evidence that Raymonda was a collector of child pornography, it was inappropriate—and heedlessly indifferent—for Agent Ouzer to rely on boilerplate language regarding the proclivities of collectors.” *Id.* The same is true here.

**Third**, the affidavit misleadingly overemphasized the importance of Bulletin Board A, suggesting a nexus between the Reece residence and Bulletin Board A that the government had no evidence to support. The affiant noted that “BULLETIN BOARD A has over 1,500 ‘approved users.’” (Ex. A, ¶ 37.) But the affidavit omits the fact that Mr. Reece was not an approved user and that, in fact, the government had no evidence that anyone using Mr. Reece’s IP address had ever even visited Bulletin Board A. A magistrate reviews a warrant application *ex parte* and relies on the government to provide not just technically true facts but an honest overall depiction of the evidentiary landscape. Here, the application’s overemphasis of Bulletin Board A’s contents and de-emphasis of the missing nexus between the Reece residence and Bulletin Board A gave the magistrate a distorted view of the government’s evidence.

**Finally**, the affidavit falsely stated that a computer located at Mr. Reece’s home “possessed and/or attempted access with intent to view child pornography *via the listed e-mail account.*” (Ex. A, ¶ 55 (emphasis added).) The government had no evidence that Mr. Reece or anyone else used any email account to access any illicit material. The reference to this phantom email account bolstered the notion that the government had established some nexus between Mr. Reece’s residence and the actual possession or accessing of child pornography when, in fact, there

was none.<sup>4</sup>

The defense respectfully submits that a *Franks* hearing is warranted on these bases.

### **CONCLUSION**

The warrant in this case was issued in contravention of the Fourth Amendment. The affidavit's only specific allegation about the Recces is consistent with someone clicking once on a hyperlink, being sent to a web address that lacked any indicia of child pornography, and declining to enter a password when prompted. The Fourth Amendment's probable cause bar is not so low. Moreover, even if the Court finds that these facts could have supported probable cause to search Mr. Reece's home in October 2015, they were stale by April of 2016. Finally, the affidavit in support of the warrant application contained misleading statements and material omissions, without which the warrant would not have issued. For all these reasons, the search of Mr. Reece's home was conducted in violation of the Fourth Amendment and suppression is appropriate.

Respectfully submitted,

LARRY REECE II

By: \_\_\_\_\_/s/\_\_\_\_\_

Amanda C. Conner, Esquire  
VSB # 88317  
Assistant Federal Public Defender  
Attorney for Larry Reece II  
Office of the Federal Public Defender  
150 Boush Street, Suite 403  
Norfolk, Virginia 23510  
(757) 457-0800  
(757) 457-0880 (telefax)  
[amanda\\_conner@fd.org](mailto:amanda_conner@fd.org)

---

<sup>4</sup> The defense is continuing to investigate the truthfulness of other facts contained in the affidavit and may request leave to supplement this Motion if other material omissions or misstatements come to light.

**CERTIFICATE OF SERVICE**

I certify that on this 31st day of October, 2016, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to:

Elizabeth Yusi  
Assistant United States Attorney  
United States Attorney's Office  
101 West Main Street, Suite 80000  
Norfolk, VA 23510  
Phone: 757-441-6331  
Fax: 757-441-6689  
[elizabeth.Yusi@usdoj.gov](mailto:elizabeth.Yusi@usdoj.gov)

\_\_\_\_\_/s/\_\_\_\_\_  
Amanda C. Conner, Esquire  
VSB # 88317  
Assistant Federal Public Defender  
Attorney for Larry Reece II  
Office of the Federal Public Defender  
150 Boush Street, Suite 403  
Norfolk, Virginia 23510  
(757) 457-0800  
(757) 457-0880 (telefax)  
[amanda\\_conner@fd.org](mailto:amanda_conner@fd.org)